IN THE CLAIMS:

Claims 1, 4, 13, 32, and 36-39 are amended herein. Claim 35 is canceled. All pending claims and their present status are produced below.

1. (Currently amended) A method of examining a network, including:

identifying an operating system of a remote host based on communications with the remote host through the network, including identifying a version and a patch level of the operating system;

identifying a service of the remote host based on communications with the remote host through the network, including identifying a version and a patch level of the service; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

2. (Previously presented) The method of claim 1, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets, and analyzing the second set of packets for inferential information indicative of the operating system;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets, wherein information contained in said third set of packets is based on information received in said second set of packets, and analyzing the fourth set of packets for inferential information indicative of the service; and

the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of packets to preexisting vulnerability information in a database.

3. (Original) The method of claim 1, wherein the step of identifying an operating system includes sending three sets of packets to the remote host and receiving three respective sets of responsive packets from the remote host.

4. (Currently amended) A method of examining a network, including:

nonintrusively ~~and reliably~~ identifying an operating system of a remote host including identifying a version of the operating system based on inferential information received from the remote host;

nonintrusively ~~and reliably~~ identifying a service of the remote host including identifying a version of the service based on inferential information received from the remote host.

5. (Original) The method of claim 4, further including:

identifying a vulnerability of the network.

6. (Original) The method of claim 4, further including:

identifying a trojan application on the host.

7. (Original) The method of claim 4, further including:

identifying unauthorized software use on the host.

8. (Original) The method of claim 4, further including:

identifying security policy violations on the network.

9. (Previously Presented) The method of claim 4, wherein:

the step of identifying an operating system further includes identifying a patch level of the operating system; and

the step of identifying a service further includes identifying a patch level of the service.

10. (Original) The method of claim 4, wherein the steps of identifying an operating system and identifying a service each includes:

sending a selected packet to the remote host;

receiving from the remote host a reflexive responsive packet.

11. (Previously Presented) The method of claim 4, wherein the steps of identifying an operating system and identifying a service each includes:

sending a plurality of selected packets to the remote host; and

receiving from the remote host a plurality of reflexive responsive packets.

12. (Previously Presented) The method of claim 4, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets; and

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets.

13. (Currently amended) A method of examining a network, including:

identifying an operating system of a remote host <u>based on communications with the remote host through the network,</u> including identifying a version of the operating system;

identifying a service of the remote host <u>based on communications with the remote host through the network,</u> including identifying a version of the service, and

identifying a vulnerability of the network <u>based on information obtained from the steps of identifying an operating system and identifying a service</u>.

14. (Original) The method of claim 13, wherein:

the step of identifying a vulnerability includes using information obtained from the steps of identifying an operating system and identifying a service to identify the vulnerability.

15. (Previously Presented) The method of claim 13, wherein:

the step of identifying an operating system further includes identifying a patch level of the operating system; and

the step of identifying a service includes identifying a patch level of the service.

16. (Previously presented) The method of claim 13, wherein the steps of identifying an operating system, identifying a service, and identifying a vulnerability each includes:

sending a selected packet to the remote host; and

receiving from the remote host a reflexive responsive packet.

17. (Previously Presented) The method of claim 13, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets; and

the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of packets to information in a database.

18. (Previously Presented) The method of claim 17, wherein:

information contained in said third set of packets is based on information received in said second set of packets; and

information contained in said fifth set of packets is based on information received in said fourth set of packets.

19. (Previously presented) A method of examining a network, including:

sending a set of selected packets to a remote host on the network;

receiving from the remote host a set of reflexive responsive packets; and

identifying conditions of the remote host by using inferential information received in the reflexive responsive packets, wherein the conditions include an operating system of the host, and a service of the host.

20. (Original) The method of claim 19, wherein the conditions further include a vulnerability of the host.

21. (Original) The method of claim 19, wherein the conditions further include the presence of unauthorized software.

22. (Original) The method of claim 19, wherein the conditions include the presence of a trojan application.

23. (Previously presented) The method of claim 19, wherein:

identifying an operating system includes identifying a version; and

identifying a service includes identifying a version.

24. (Previously presented) The method of claim 19, wherein:

identifying an operating system includes identifying a version and a patch level; and

identifying a service includes identifying a version and a patch level.

25. (Previously Presented) The method of claim 19, wherein

the step of sending a set of selected packets to a host on the network includes sending a plurality of sets of packets to the host; and

the step of receiving from the remote host a set of reflexive responsive packets includes receiving a like plurality of sets of reflexive responsive packets.

26. (Previously presented) A method of detecting a vulnerability of a network, comprising:

sending a first set of test packets to a remote host on the network;

receiving a first set of reflexive packets from the remote host in response to the first set of test packets;

sending a second set of test packets to the remote host on the network, wherein information contained in the first set of test packets is based on inferential information contained in the first set of reflexive packets;

receiving a second set of reflexive packets from the remote host in response to the second set of test packets;

based on inferential information contained in the first set of reflexive packets, identifying an operating system of the remote host, including a version and a patch level; and

based on inferential information contained in the second set of reflexive packets, identifying a service of the remote host, including a version and a patch level.

27. (Previously presented) The method of claim 26, further including:

sending a seventh set of selected packets to a host on the network;

receiving an eighth set of packets from the remote host in response to the seventh set of packets;

sending a ninth set of selected packets to a host on the network;

receiving a tenth set of packets from the remote host in response to the ninth set of packets; and

based on information contained in the eight and tenth sets of packets, identifying a service of a host on the network, including a version and a patch level.

28. (Original) The method of claim 27, further including:

based on information contained in at least the tenth sequence, identifying a vulnerability.

29. (Previously presented) The method of claim 26, wherein:

the first set of packets includes:

a SYN Packet with false flag in the TCP option header;

a Fragmented UPD packet with malformed header (any header inconsistency is sufficient), where the packet is 8K in size;

a FIN Packets of a selected variable size or a FIN packet without the ACK or SYN flag properly set; and

a generic, well-formed ICMP ECHO request packet;

the third set of packets includes:

a generic well-formed TCP Header set to 1024 bytes in size;

a Packet requesting an ICMP Timestamp;

a Packet with min/max segment size set to a selected variable value; and

a UPD packet with the fragment bit set;

the fifth set of packets includes:

a TCP Packet with the header and options set incorrectly;

a well-formed ICMP Packet;

a Fragmented TCP or UPD packet;

a packet with an empty TCP window or a window set to zero;

a generic TCP Packet with 8K of random data; and

a SYN Packet with ACK and RST flags set.

30. (Previously presented) A method of examining a network, comprising:

sending a plurality of packets to a host on the network;

receiving a responsive plurality of packets from the host;

comparing inferential information in the responsive packets to information stored in a database; and

based on the comparison, identifying a plurality of network conditions, including a vulnerability of the network.

31. (Previously presented) A method of examining a network, comprising:

sending packets to a host on the network;

receiving responsive packets from the host;

comparing inferential information in the responsive packets to information stored in a database; and

based on the comparison, identifying a trojan application on the network.

32. (Currently amended) A method of examining a network, comprising:

sending packets to a host on the network;

receiving responsive packets from the host;

comparing inferential information in the responsive packets to information stored in a database; and

based on the comparison, identifying unauthorized software use on the network host.

33. (Previously presented) A method of examining a network, comprising:

sending packets to a host on the network;

receiving responsive packets from the host;

comparing inferential information in the responsive packets to information stored in a database; and

based on the comparison, inferring an unknown vulnerability.

34. (Previously presented) A method of examining a network, comprising:

sending packets to a host on the network;

receiving responsive packets from the host;

comparing inferential information in the responsive packets to information stored in a database; and

based on the comparison, identifying a security policy violation.

35. (Canceled)

36. (Currently amended) ~~The system of claim 35,~~ A system for examining a network, comprising:

a database including a set of reflex signatures;

a packet generator;

a comparison unit in communication with the packet generator and the database;

wherein the packet generator is designed to generate and transmit a plurality of test packets to the network;

wherein the comparison unit is designed to receive responsive packets from the network and to compare inferential information from the reflex signatures; and

wherein the comparison unit is further designed to identify a vulnerability in the network based on its comparison of packet information with reflex signatures.

37. (Currently amended) The system of claim 36 ~~35~~, wherein the comparison unit is further designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

38. (Currently amended) The system of claim 36 ~~35~~, wherein the comparison unit is designed to provide information to the packet generator, and wherein the packet generator is designed to use the information to selectively generate packets.

39. (Currently amended) A computer readable medium, having instructions stored therein, which, when executed by a computer, causes the computer to perform the steps of:

identifying an operating system of a remote host based on communications with the remote host through the network, including identifying a version of the operating system;

identifying a service on the port and a service of the remote host based on communications with the remote host through the network, including identifying a version of the service; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

40. (Original) The computer readable medium of claim 39, wherein:

the instructions for identifying an operating system further include instructions for identifying a patch level of the operating system; and

the instructions for identifying a service further include instructions for identifying a patch level of the service.

41. (Previously Presented) The computer readable medium of claim 39, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets, wherein information contained

in said third set of packets is based on information received in said second set of packets; and

the step of identifying a vulnerability includes comparing information contained in the second sequence of packets and the fourth sequence of packets to information in a database.

42. (Previously presented) A method for use by a host on a network, comprising:

receiving a set of selected packets from remote equipment; and

automatically sending a second set of packets to said remote equipment, the second set of packets including inferential information that enables the remote equipment to identify a vulnerability on the network.

43. (Previously presented) A method for use by a host on a network, comprising:

receiving a first set of test packets from remote equipment;

automatically sending a first set of reflexive packets to said remote equipment, the first set of reflexive packets containing information generated according to a Request For Comment (RFC) protocol and indicative of an operating system, including a version and patch level;

receiving a first test packet from remote equipment;

automatically sending a second set of reflexive packets to said remote equipment, the second set of reflexive packets containing information generated according to a Request For Comment (RFC) protocol and indicative of a service, including a version and patch level;

wherein the first set of reflexive packets includes information that enables the remote equipment to identify the operating system on the host, including a version and a patch level;

wherein the second set of reflexive packets includes information that enables the remote equipment to identify the service on the host, including a version and a patch level.

44. (Previously Presented) A method of examining a network, including:

identifying an operating system of a remote host, including a version and a patch level of the operating system with a first set of packets, the first set of packets comprising an operating system packet to determine the operating system, an operating system version packet to determine the operating system version based on the determined operating system, and an operating system patch level packet to determine the operating system patch level based on the determined operating system version;

identifying a service of the remote host, including a version and a patch level of the service with a second set of packets based on at least one of the first set of packets, the first set of packets comprising a service packet to determine the service, a service version packet to determine the service version based on the determined service, and a service patch level packet to determine the service patch level based on the determined service version; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

45. (Previously Presented) A method of examining a network, including:

identifying an operating system of a remote host, including a version and a patch level of the operating system, with responses to nonconforming data packets;

identifying a service of the remote host, including a version and a patch level of the service with responses to nonconforming data packets; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.